

REMARKS

Apparatus Claims 25 through 36 are added to more clearly define the scope of the Applicant's invention. Such claims are supported by the application as filed and without the addition of new matter. Thus, by this Amendment, Claims 1 through 36 are presented for examination.

Applicant's attorney's check in the amount of \$695 is enclosed to cover the filing charges associated with the twelve (12) additional claims presented herein as well as the RCE filing fee.

The Examiner has restated pending rejections of the method claims. Claims 1 through 16, 21 and 23 are rejected as allegedly rendered obvious by the International application of Schultz et al. in view of the United States patent of Carter. Claims 17 through 20 and 22 are rejected are rejected as allegedly obvious on the basis of the foregoing combination further in view of the United States patent of Chen et al. Finally, Claim 24 is rejected as obvious on the basis of Schultz et al. in view of Carter further in view of the United States patent of Auerbach et al.

It will be clear from the apparatus claims presented herewith and from the arguments that follow that the present invention represents an entirely different approach to the provision of a patient-subscriber's medical (or other) records to medical personnel over a network. As a result, all presently-pending claims of the application, method as well as apparatus, define patentable subject matter.

Both the claimed invention and the Schultz reference are directed to providing patient-subscriber data for accessing over an electronic network. In the claimed invention, a plurality of data area access systems or secure data memories (e.g. a doctor's office) are provided, along with, and separate from, an information center. Patient data is stored at the data access system where such data was generated. A record of the existence and location of such patient data (i.e., the particular data area access system where it is stored) is transmitted to and kept at the information center. The data owner (i.e. the patient), informs the information center of the identities of the third party professionals (data area access systems) entitled to access to the data stored at other data access systems (and authorizes data access systems to store generated data), providing the third party professional the access necessary to

review such data, thereby preventing the duplication of medical data (e.g. taking of unnecessary additional x-rays) within the network.

Once a request for patient records is received at the information center from a data area access system, the information center, upon verification of the request, will provide information indicating the existence of medical records (but not the underlying data, such as x-rays) upon verification of a data area access system user code. The information provided by the information center to the qualified data area access system will include the identity of the data area access systems where particular patient information is stored. Figure 5 of the application and the accompanying written description illustrate the process whereby data transfer within the invention proceeds among data area access systems subject to continuous user verification steps. Such step-by-step verification, and the consequent high security, follows from a combination of the arrangement and protocols of the claimed invention.

In contrast to the system of the claimed invention wherein data is stored where it is generated (data access system) for sharing with other third party data access systems upon

approval by the patient-subscriber, Schultz et al. merely provides an electronic medical record that is accessible over a network. The electronic record permits a traveler to more-or-less take his or her medical records along with him/her so that a foreign treating doctor may have access to the medical history of the otherwise-unknown patient. Such data, in the form of a GEMR (Global Electronic Medical Record) 100 is stored on a GEMR server 55 and is accessible by navigation of the patient-subscriber's GEMR home page 111 subject to provision of network address and password information to the third party (e.g. treating physician).

The patient-subscriber is responsible for the entry of personal medical information and records onto his or her GEMR 100. That is, he or she must obtain his or her personal medical data for it to be accessible to third part physicians via access to the GEMR ("Note that access to these files/databases within (or through) the institutional server(s) 75', because of security reasons associated with the institutional server(s) 75', may require that the subscriber obtain permission, for example, by application to authorities in control of the institutional server(s) 75' at the time of subscribing to the GEMR. With such permission, or if no permission is required, a subscriber may be

able to access (or make additional linkage to) the institutional server(s) 75' as described above and copy information stored in (or gain access to information through) the institutional server(s) 75' which is associated with the GEMR 100 and the link blocks 121-128. The scope of the present invention encompasses the ability for the subscriber to obtain permission, if required, from the authorities in control of the information stored in (or obtained through) the institutional server(s) 75' in order to obtain that information associated with the link blocks 121-128." Schultz et al, p. 24, lines 18 through 30.)

Method Claim 1 and the claims that depend therefrom are directed to a method for secured access to data in a network including an information center and a plurality of data area access systems in which permission to store said data and to define, at the information center, access rights of third parties to said data is limited to the owner of rights to said data. Such method includes, among other limitations, "in each case storing the data only once in one of said data area access systems not accessible to the owner of the rights".

Schultz et al. includes no teaching that would suggest that data is stored only once (i.e. at the originating data area

access system). Rather, it follows from the provision of the GEMR server 55 (or 55') as illustrated in Figure 1 that data is stored not only where it is generated but also on a GEMR server 55 or 55'. The Examiner is entirely incorrect when denying Applicant's argument in support of patentability based upon the claim limitation of storage "only once". The references to Schultz et al. (P. 2, lines 28 through 30 and p. 3, lines 12 through 14) that the Examiner cites in rejecting Applicant's attorney's argument in support of patentability on this point should be reconsidered as those portions of Schultz et al. do not in fact support, or even relate to, refutation of Applicant's attorney's argument for patentability.

Additionally, in the claimed invention (as set forth in the other underlined portion of the limitation of the method cited above, the subscriber-owner of data only acts to provide or deny access to requests for data from area access systems (e.g. doctors' offices). This is done by communication between the subscriber-owner and the information center which contains a list of the data stored at the various area access systems (but not the data itself, unlike the GEMR servers of Schultz et al.) The system of the claimed invention functions without owner-subscriber access to the data itself. This is entirely unlike

Schultz et al. in which the subscriber-owner inputs data at a network address wherein his or her GEMR home page 111 provides a platform from which an authorized physician may navigate to locate the medical data that the patient (subscriber-owner) has obtained and provided. In contrast, in the method of the claimed invention, the subscriber-owner is "blind" with regard to the content of the medical data to which he or she provides or denies access.

Apparatus Claim 25 and the claims that depend therefrom are directed to a system in which, while "display and modification of the information defining the access rights to said entered piece of data is restricted to said authorized user of said information center", "access to any piece of data entered into the system is restricted to those authorized users of the system having appropriate access rights as defined by said information for the piece of data to be accessed". No reference is made in the method claims to any access rights of the subscriber-owner to his or her data. This is entirely consistent with the method claims for reasons discussed above. The role of the owner of the data (e.g. patient) is limited in the claimed invention to the designation of authorized users of his or her data. The subscriber-owner is not an authorized user of his or

her data. This is entirely unlike the configuration of Schultz et al. in which "authorized user" and "subscriber" are employed interchangeably. (See, for example, in the Abstract, "Systems and methods for a secure, confidential, subscriber-driven and updatable Global electronic Medical Record (GEMR) are provided which is network-based and includes linked subscriber medical information with access limited by network address and password only to the subscriber or an authorized user...") The owner of the data does not possess access rights to his/her own data in the claimed invention. This is consistent with real life in which it is the physician's role to advise a patient of the implications of the patient's medical data and patient access to raw medical data is of no real therapeutic benefit and, in fact, might prove to be unnecessarily alarming to a layman patient.



For the foregoing reasons, all presently-pending claims define patentable subject matter. Prompt allowance and issuance of all such claims are therefore earnestly solicited.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Elliott N. Kramsky", written in a cursive style.

Elliott N. Kramsky  
Registration No. 27,812  
Attorney for Applicant  
5850 Canoga Avenue, Suite 400  
Woodland Hills, CA 91367  
Ph: (818) 992-5221  
Fx: (818) 710-2751